OIPE JC139 MAR 18 2002 PATENT & TRADEMARK OFFICE

2600 #2 7-9-02 cl 2430

520.41277X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

2635

Applicant(s): SHIMADA

Serial No.: 10 / 081,204

Filed: FEBRUARY 25, 2002

Title: PREDECESSOR AND SUCCESSOR TYPE MULTIPLEX SYSTEM

LETTER CLAIMING RIGHT OF PRIORITY

RECEIVED
APR 2 3 2002
Technology Center 2600

Assistant Commissioner for Patents
Washington, D.C. 20231

MARCH 18, 2002

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 2001-195687
Filed: JUNE 28, 2001

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/rp
Attachment

NT 0605

OIPE JC139 MAR 18 2002 PATENT & TRADEMARK OFFICE

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ６月２８日

出願番号
Application Number: 特願２００１－１９５６８７

[ST.10/C]: [ＪＰ２００１－１９５６８７]

出願人
Applicant(s): 株式会社日立製作所

RECEIVED
APR 23 2002
Technology Center 2600

２００２年 ３月 １日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００２－３０１１６６５

【書類名】　特許願
【整理番号】　H01004461A
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 11/18
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　島田　健太郎
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【電話番号】　03-3212-1111
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　追走型多重化システム、及び追走により信頼性を高めるデータ処理方法

【特許請求の範囲】

【請求項１】

まったく同一な先行系、後続系の二つの系、および、入力データを前記後続系に入力するまで一時記憶する入力データ一時記憶手段、前記先行系からの出力データを一時記憶する出力データ一時記憶手段、前記後続系の出力データと前記出力データ一時記憶手段に記憶された前記先行系の出力データを比較する出力データ比較手段、前記出力データ比較手段の結果によって前記後続系の出力データを外界に出力するかどうか制御する出力データゲート手段、前記先行系が入力された入力データに対し正常に動作することを確認して前記後続系の動作を開始することを制御する先行後続動作制御手段を備える２重化システム。

【請求項２】

まったく同一なn個(nは3以上)の系１～系ｎ、及び入力データを前記系2～系ｎに入力するまで一時記憶する入力データ一時記憶手段、及び前記系１～系n-1の出力データを一時記憶する出力データ一時記憶手段、前記系２～系nの出力データと出力データ一時記憶手段に記憶された前記系１～系n-1の出力データを比較する出力データ比較手段、前記出力データ比較手段の結果によって前記系ｎの結果を外界に出力するかどうか制御する出力データゲート手段、前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段を備える多重化システム。

【請求項３】

請求項２に記載された多重化システムであって、前記入力データ一時記憶手段が系2～系ｎ毎にn-1個の系別入力データ一時記憶手段から構成され、前記出力データ一時記憶手段が系１～系n-1毎にn-1個の系別出力データ一時記憶手段から構成され、前記出力データ比較手段が、前記系m(mは1からn-1まで整数)の系別出力データ一時記憶手段に記憶された出力データと前記系m+1の出力データの比較を行うn-1個の系別出力データ比較手段と、前記n-1個の系別出力データ比較手段のn-

1個の出力結果を順々に集計する出力データ比較結果集計手段から構成される多重化システム。

【請求項４】

請求項１に記載の２重化システムであって、前記先行系が異常動作したことを通知する異常動作通知手段を備え、前記先行後続動作制御手段が、前記異常動作通知手段により通知される異常動作通知に基づき前記後続系の動作の開始の制御を行う後続系開始制御手段を含むことを特徴とする２重化システム。

【請求項５】

請求項２に記載の多重化システムであって、前記系1～系n-1がそれぞれ異常動作したことを通知する異常動作通知手段を備え、前期先行後続動作制御手段が、前記系m(mは１からn-1までの整数)が備える前記異常動作通知手段により通知される異常動作通知に基づき前記系m+1の動作の開始の制御をそれぞれ行うn-1個の後続系開始制御手段を含むことを特徴とする多重化システム。

【請求項６】

請求項４に記載の２重化システムであって、更に、前記異常動作通知手段により前記先行系の異常動作が通知されたとき、前記後続系の状態を前記先行系へ複写し、前記先行系の状態を前記後続系の状態と同一にして回復することのできる状態複写回復手段を備える２重化システム。

【請求項７】

請求項５に記載の多重化システムであって、更に、前記異常動作通知手段により前記系m（mは１からn-1の整数）の異常動作が通知されたとき、前記系m+1の状態を前記系mへ複写し、前記系ｍの状態を前記系m+1の状態と同一にして回復することのできる状態複写回復手段をn-1個備える多重化システム。

【請求項８】

請求項６に記載の２重化システムであって、更に、前記異常動作通知手段により前記先行系の異常動作が通知され、前記状態複写回復手段により前記先行系の状態を回復した後、前記入力データー時記憶手段に記憶した入力データを前記先行系に再び入力して再度動作させるデータ再入力実行手段を備える２重化システム。

【請求項９】

請求項７に記載の多重化システムであって、更に、前記異常動作通知手段により前記系m（mは１からn-1の整数）の異常動作が通知され、前記状態複写回復手段により前記系ｍの状態を回復した後、前記入力データ一時記憶手段に記憶した入力データを前記系mに再び入力して再度動作させるデータ再入力実行手段を備える多重化システム。

【請求項１０】

請求項２に記載の多重化システムであって、更に、前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶した系m(mは１からn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記系m+2の状態を前記系m及び前記系m+1に複写して、前記系m及び前記系m+1の状態を前記系m+2の状態と同一することの出来る状態複写回復手段を備える多重化システム。

【請求項１１】

請求項１０に記載の多重化システムであって、更に、前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶した系m(mは１からn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記状態複写回復手段により前記系m及び前記系m+1の状態を回復した後、前記入力データ一時記憶手段に記憶した入力データを前記系m及び系m+1に再び入力して再度動作させるデータ再入力実行手段を備える多重化システム。

【請求項１２】

まったく同一なn個(nは3以上)の系１～系ｎ、及び入力データを前記系2～系ｎに入力するまで一時記憶する入力データ一時記憶手段、及び前記系１～系n-2の出力データを一時記憶する出力データ一時記憶手段、前記系２～系n-1の出力データと出力データ一時記憶手段に記憶された前記系１～系n-2の出力データを比較する出力データ比較手段、前記出力データ比較手段の結果によって前記系n-1の結果を外界に出力するかどうか制御する出力データゲート手段、前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段、前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶された前記系m(mは１か

らn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記系m+2の状態を前記系m及び前記系m+1に複写して、前記系m及び前記系m+1の状態を前記系m+2の状態と同一することの出来る状態複写回復手段を備える多重化システム。

【請求項１３】

請求項１２に記載の多重化システムであって、更に、前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶した系m(mは１からn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記状態複写回復手段により前記系m及び前記系m+1の状態を回復した後、前記入力データ一時記憶手段に記憶した入力データを前記系m及び系ｍ+1に再び入力して再度動作させるデータ再入力実行手段を備える多重化システム。

【請求項１４】

請求項４に記載の２重化システムであって、前記異常動作通知手段が、前記先行系が結果を一定時間内に出力しないかどうかで異常動作することを検出する出力タイムアウト検知手段を含むことを特徴とする２重化システム。

【請求項１５】

請求項５に記載の多重化システムであって、前記異常動作通知手段が、前記系1～系n-1がそれぞれ結果を一定時間内に出力しないかどうかで異常動作することを検出する出力タイムアウト検知手段を含むことを特徴とする多重化システム。

【請求項１６】

請求項４に記載の２重化システムであって、更に、前記先行後続動作制御手段が、前記異常動作通知手段により前記先行系の異常動作が通知されたとき前記後続系の動作を継続させ、前記先行系からの出力を前記出力データ比較手段により比較することを停止し、前記出力データゲート手段が前記後続系の出力データを外界にそのまま出力するように制御を行う縮退運転制御手段を含むことを特徴とする２重化システム。

【請求項１７】

請求項５に記載の多重化システムであって、更に、前記先行後続動作制御手段が、前記異常動作通知手段により前記系1～系n-1のうちの１個の系の異常動作が通

知されたとき、前記系１～nのうちの異常動作が通知されていない系の動作を継続させ、前記異常動作が通知された系からの出力を前記出力データ比較手段により比較することを停止し、前記出力データゲート手段が前記異常動作が通知された系からの出力の比較結果の有無に関わらず前記系ｎの結果を外界に出力するよう制御を行う縮退運転制御手段を含むことを特徴とする多重化システム。

【請求項１８】

請求項１に記載の２重化システムであって、更に、前記後続系が異常動作したことを検出する後続系異常動作検出手段と、前記後続系異常動作検出手段により前記後続系の異常動作が検出されたとき、前記先行系の状態を前記後続系へ複写し、前記後続系の異常動作の回復を行う後続系障害回復手段を備える２重化システム。

【請求項１９】

請求項２に記載の多重化システムであって、更に、前記系ｒ（ｒは２からnの整数）が異常動作したことを検出する後続系異常動作検出手段と、前記後続系異常動作により前記系ｒの異常動作が検出されたとき、系r-1の状態を前記系ｒへ複写し、前記系ｒの異常動作の回復を行う後続系障害回復手段を備える多重化システム。

【請求項２０】

入力データから第1の出力結果を求める第1のステップと、前記第1の出力結果が障害なく得られることを確認する第２のステップと、前記第２のステップにおいて前記第１の結果が障害なく得られたことが確認できたとき、再び前記入力データから第２の出力結果を求める第３のステップと、前記第２の出力結果が障害なく得られることを確認する第４のステップと、前記第４のステップにおいて前記第２の出力結果が障害なく得られたことが確認できたとき、前記第1の出力結果と前記第２の出力結果を比較する第５のステップと、前記第５のステップにおいて、前記第1の出力結果と前記第２の出力結果が比較した結果同一であれば、前記第１または第２の出力結果を外部へ出力する第６のステップからなるデータ処理方法。

【請求項２１】

請求項２０に記載の方法であって、更に、前記第２のステップにおいて、前記第１の出力結果が障害なく得られたことが確認できなかったとき、前記第１のステップに戻って第１の出力結果を再び求め直すことが出来るように準備を行い、第１のステップに戻る第７のステップを備えるデータ処理方法。

【請求項２２】

請求項２０に記載の方法であって、更に、前記第４のステップにおいて、前記第２の出力結果が障害なく得られたことが確認できなかったとき、前記第３のステップに戻って第２の出力結果を再び求め直すことが出来るように準備を行い、第３のステップに戻る第８のステップを備えるデータ処理方法。

【請求項２３】

請求項２１に記載の方法であって、更に、前記第２のステップにおいて第１の出力が障害なく得られたことが確認できなかったとき、予め定める一定回数ｋ回(ｋは１以上)だけ第７のステップに移って準備を行うよう回数を数える第９のステップを含むデータ処理方法。

【請求項２４】

請求項２２に記載の方法であって、更に、前記第４のステップにおいて第２の出力が障害なく得られたことが確認できなかったとき、予め定める一定回数ｊ回(ｊは１以上)だけ第８のステップに移って準備を行うよう回数を数える第１０のステップを含むデータ処理方法。

【請求項２５】

請求項２０に記載の方法であって、更に、前記第５のステップにおいて、前記第１の出力結果と前記第２の出力結果を比較した結果同一でなければ、前記第１のステップに戻って前記第１の出力結果と前記第２の出力結果を再び求め直すことが出来るように準備を行い、第１のステップに戻る第１１のステップを備えるデータ処理方法。

【請求項２６】

請求項２５に記載の方法であって、更に、前記第５のステップにおいて、前記第１の出力結果と前記第２の出力結果を比較した結果同一でなければ、予め定める一定回数ｓ回(ｓは１以上)だけ前記第１１のステップに移って準備を行うよう回

数を数える第１２のステップを含むデータ処理方法。

【請求項２７】

まったく同一なn個(nは２以上)の系１～系ｎと、入力データを前記系2～系ｎに入力するまで一時記憶する入力データー時記憶手段と、前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段と、前記系１～系n-1が異常動作したことを通知する異常動作通知手段を備え、前記先行後続動作制御手段が、前記系m(mは１からn-1までの整数)が備える前記異常動作通知手段により通知される異常動作通知に基づき前記系m+1の動作の開始の制御をそれぞれ行うn-1個の後続系開始制御手段を含むことを特徴とする多重化システム。

【請求項２８】

請求項２７に記載の多重化システムであって、前記異常動作通知手段により前記系m（mは１からn-1の整数）の異常動作が通知されたとき、前記系m+1の状態を前記系mへ複写し、前記系ｍの状態を前記系m+1の状態と同一にして回復することのできる状態複写回復手段をn-1個備える多重化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータ・システム等の、入力データから一定の出力データを得るシステムの信頼性を高める技術に属し、特にソフトウェアを含めてシステム全体の信頼性を高める技術に関する。

【０００２】

【従来の技術】

従来、システムの信頼性を高める技術としては、同一なシステム(系)を２個用意し、これを同時に動作させ、同時に出力される結果を比較することによって、出力結果の信頼性を高める技術が用いられてきた。例えば特開平9-198124はこのような２重化システムの例である。２個の同一な系とそれぞれの系からの出力を比べて誤りがないかどうかを判定する判定部を持ち、２個の系を同時に動作させる。

【０００３】

このような２重化システムでは、２個の系が同時に動作を開始するため、誤りが検出された時点では両方の系とも系内の状態が動作することにより変化している。従って、障害回復のためには両方の系の状態復旧処理が必要である。更にこの状態復旧処理には復旧すべき系の状態を記録しておくことなどが必要であり、記録するためには新たに記録装置等が必要となる。

【０００４】

また先の例、特開平9-198124は、１個の系内においても障害検出を行う手段を備えている。しかし、２個の系とも同時に動作を開始しており、２個の系とも状態が変化しているため、片方の１個において障害が検出されても、状態復旧のための状態記録は必要である。

【０００５】

特開平9-198124では１個の系内の障害検出は、１個の系を２回動作されることにより行っている。特開平9-198124はアナログ・データの入力に対して動作するシステムを想定しており、２回動作させることで雑音等による障害の検出を目的としている。しかし一般のディジタル・コンピュータ・システムのようなディジタル・システムはディジタル信号であるので雑音等に強く、１個の系が２回動作することで障害検出を行おうとしても困難である。

【０００６】

２重化システムにおいて、システムがディスク装置である場合には、障害を起こした系に他方の障害を起こしていない系の状態(ディスクに記憶されたデータ)を複写して回復することが可能である。特開平10-3396はこのような例である。しかし、一般的なコンピュータ・システムの場合には、系の状態としてはディスクに記憶されたデータ以外にも主記憶(メインメモリ)の内容などがある。これら主記憶の内容等は、２個の系が同時に動作を開始しているため、一方の系で障害が検出された時には既に他方の系は、変更中の中間的な状態となっている。従って他方の系から障害を起こした系に一定の状態を複写して状態回復を行うことは難しい。

【０００７】

２重化システムの構成法においては、システムがコンピュータ・システムである場合には、ソフトウェアでプログラムを同一の入力データで２回実行することにより、信頼性に関し２重化することと同じ効果を得ようとする従来技術も存在する。特開平8-328888はこのような従来技術の例である。しかし、先にも述べたように、コンピュータ・システムのようなディジタル・システムはディジタル信号であるので雑音等に強く、１個の系が２回動作することで信頼性を高めようとするのは、効果が小さい。特開平8-328888では、記憶装置を共有する複数の情報処理装置(複数の系)を用いた場合、プログラムの２回の実行をそれぞれ別々の情報処理装置に分散してシステム全体の負荷を分散して性能を上げる記述があり、その場合では複数の系でプログラムが実行されることになる。しかし、初回の実行の正常終了を確認すること、及び障害終了時にこれを検知することについては技術の開示がなく、初回実行時にソフトウェア障害を含む障害を検知することは不可能であり、初回実行時の障害回復も行えない。さらに別々の系で２回実行した結果、出力が不一致であったとき、２個の系の状態を回復して再実行させることについても技術の開示がなく、不可能である。

【０００８】

【発明が解決しようとする課題】

本発明は２重化システムあるいは３個以上の系を持つ多重化システムにおいて、障害を起こしたシステムの状態を正しく回復させることを課題とする。また特にシステムがコンピュータ・システムである場合に、ハードウェアの障害や誤動作に加え、ソフトウェアの不良を含むソフトウェア障害についても正しく状態回復を行うことを課題とする。またソフトウェアの不良を含むソフトウェア障害についても、システムの動作を継続させることを課題とする。

【０００９】

【課題を解決するための手段】

本発明による多重化システムでは、上記の課題を解決するために、

まったく同一な先行系、後続系の二つの系と、

入力データを前記後続系に入力するまで一時記憶する入力データ一時記憶手段と、

前記先行系からの出力データを一時記憶する出力データ一時記憶手段と、

前記後続系の出力データと前記出力データ一時記憶手段に記憶された前記先行系の出力データを比較する出力データ比較手段と、

前記出力データ比較手段の結果によって前記後続系の出力データを外界に出力するかどうか制御する出力データゲート手段と、

前記先行系が入力された入力データに対し正常に動作することを確認して前記後続系の動作を開始することを制御する先行後続動作制御手段を備える。

【００１０】

また、まったく同一なn個(nは3以上)の系１～系ｎと、

入力データを前記系2～系ｎに入力するまで一時記憶する入力データ一時記憶手段と、

前記系１～系n-1の出力データを一時記憶する出力データ一時記憶手段と、

前記系２～系nの出力データと出力データ一時記憶手段に記憶された前記系１～系n-1の出力データを比較する出力データ比較手段と、

前記出力データ比較手段の結果によって前記系ｎの結果を外界に出力するかどうか制御する出力データゲート手段と、

前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段を備える。

【００１１】

更に、前記入力データ一時記憶手段が系2～系ｎ毎にn-1個の系別入力データ一時記憶手段から構成され、

前記出力データ一時記憶手段が系１～系n-1毎にn-1個の系別出力データ一時記憶手段から構成され、

前記出力データ比較手段が、前記系m(mは1からn-1まで整数)の系別出力データ一時記憶手段に記憶された出力データと前記系m+1の出力データの比較を行うn-1個の系別出力データ比較手段と、前記n-1個の系別出力データ比較手段のn-1個の出力結果を順々に集計する出力データ比較結果集計手段から構成される。

【００１２】

また、前記先行系が異常動作したことを通知する異常動作通知手段を備え、

前記先行後続動作制御手段が、前記異常動作通知手段により通知される異常動作通知に基づき前記後続系の動作の開始の制御を行う後続系開始制御手段を備える。

【００１３】

また、前記系1～系n-1がそれぞれ異常動作したことを通知する異常動作通知手段を備え、

前期先行後続動作制御手段が、前記系m(mは１からn-1までの整数)が備える前記異常動作通知手段により通知される異常動作通知に基づき前記系m+1の動作の開始の制御をそれぞれ行うn-1個の後続系開始制御手段を備える。

【００１４】

更に、前記異常動作通知手段により前記先行系の異常動作が通知されたとき、前記後続系の状態を前記先行系へ複写し、前記先行系の状態を前記後続系の状態と同一にすることのできる状態複写回復手段を備える。

【００１５】

また、前記異常動作通知手段により前記系m（mは１からn-1の整数）の異常動作が通知されたとき、前記系m+1の状態を前記系mへ複写し、前記系ｍの状態を前記系m+1の状態と同一にすることのできる状態複写回復手段をn-1個備える。

【００１６】

更に、前記出力データ比較手段の結果が不一致であった時に、前記入力データ一時記憶手段に記憶した入力データを前記先行系に再び入力して再度動作させるデータ再入力実行手段を備える。

【００１７】

また、前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶した系m（mは１からn-1までの整数）の出力データと、前記系m+1の出力データが不一致であった時に、前記入力データ一時記憶手段に記憶した入力データを前記系mに再び入力して再度動作させるデータ再入力実行手段を備える。

【００１８】

更に、前記出力データ比較手段の結果において、前記出力データ一時記憶手段

に記憶した系m(mは１からn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記系m+2の状態を前記系m及び前記系m+1に複写して、前記系m及び前記系m+1の状態を前記系m+2の状態と同一することの出来る状態複写回復手段を備える。

【００１９】

また、まったく同一なn個(nは3以上)の系１～系ｎと、

入力データを前記系2～系ｎに入力するまで一時記憶する入力データ一時記憶手段と、

前記系１～系n-2の出力データを一時記憶する出力データ一時記憶手段と、

前記系２～系n-1の出力データと出力データ一時記憶手段に記憶された前記系１～系n-2の出力データを比較する出力データ比較手段と、

前記出力データ比較手段の結果によって前記系n-1の結果を外界に出力するかどうか制御する出力データゲート手段と、

前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段と、

前記出力データ比較手段の結果において、前記出力データ一時記憶手段に記憶された前記系m(mは１からn-2までの整数)の出力データと、前記系m+1の出力データが不一致であった時、前記系m+2の状態を前記系m及び前記系m+1に複写して、前記系m及び前記系m+1の状態を前記系m+2の状態と同一することの出来る状態複写回復手段を備える。

【００２０】

また、前記異常動作通知手段が、前記先行系が結果を一定時間内に出力しないかどうかで異常動作することを検出する出力タイムアウト検知手段を含む。

【００２１】

また、前記異常動作通知手段が、前記系1～系n-1がそれぞれ結果を一定時間内に出力しないかどうかで異常動作することを検出する出力タイムアウト検知手段を含む。

【００２２】

更に、前記先行後続動作制御手段が、前記異常動作通知手段により前記先行系

の異常動作が通知されたとき前記後続系の動作を継続させ、前記先行系からの出力を前記出力データ比較手段により比較することを停止し、前記出力データゲート手段が前記後続系の出力データを外界にそのまま出力するように制御を行う縮退運転制御手段を含む。

【００２３】

また、前記先行後続動作制御手段が、前記異常動作通知手段により前記系1～系n-1のうちの１個の系の異常動作が通知されたとき、前記系１～nのうちの異常動作が通知されていない系の動作を継続させ、前記異常動作が通知された系からの出力を前記出力データ比較手段により比較することを停止し、前記出力データゲート手段が前記異常動作が通知された系からの出力の比較結果の有無に関わらず前記系ｎの結果を外界に出力するよう制御を行う縮退運転制御手段を含む。

【００２４】

更に、前記後続系が異常動作したことを検出する後続系異常動作検出手段と、

前記後続系異常動作検出手段により前記後続系の異常動作が検出されたとき、前記先行系の状態を前記後続系へ複写し、前記後続系の異常動作の回復を行う後続系障害回復手段を備える。

【００２５】

また、前記系ｒ（ｒは２からnの整数）が異常動作したことを検出する後続系異常動作検出手段と、

前記後続系異常動作により前記系ｒの異常動作が検出されたとき、系r-1の状態を前記系ｒへ複写し、前記系ｒの異常動作の回復を行う後続系障害回復手段を備える。

【００２６】

また、まったく同一なn個（nは２以上）の系１～系ｎと、入力データを前記系2～系ｎに入力するまで一時記憶する入力データ一時記憶手段と、前記系１～系n-1が入力された入力データに対し正常に動作することを確認して前記系２～系ｎの動作を開始することを制御する先行後続動作制御手段を備える。

【００２７】

また本発明による信頼性を高める方法では、入力データから第1の出力結果を

求める第1のステップと、前記第1の出力結果が障害なく得られることを確認する第２のステップと、前記第２のステップにおいて前記第１の結果が障害なく得られたことが確認できたとき、再び前記入力データから第２の出力結果を求める第３のステップと、前記第２の出力結果が障害なく得られることを確認する第４のステップと、前記第４のステップにおいて前記第２の出力結果が障害なく得られたことが確認できたとき、前記第1の出力結果と前記第２の出力結果を比較する第５のステップと、前記第５のステップにおいて、前記第1の出力結果と前記第２の出力結果が比較した結果同一であれば、前記第１または第２の出力結果を外部へ出力する第６のステップからなる。

【００２８】

更に、前記第２のステップにおいて、前記第１の出力結果が障害なく得られたことが確認できなかったとき、前記第１のステップに戻って第１の出力結果を再び求め直すことが出来るように準備を行い、第１のステップに戻る第７のステップを備える。

【００２９】

更に、前記第４のステップにおいて、前記第２の出力結果が障害なく得られたことが確認できなかったとき、前記第３のステップに戻って第２の出力結果を再び求め直すことが出来るように準備を行い、第３のステップに戻る第８のステップを備える。

【００３０】

更に、前記第２のステップにおいて第１の出力が障害なく得られたことが確認できなかったとき、予め定める一定回数ｋ回（ｋは１以上）だけ第７のステップに移って準備を行うよう回数を数える第９のステップを備える。

【００３１】

更に、前記第４のステップにおいて第２の出力が障害なく得られたことが確認できなかったとき、予め定める一定回数ｊ回（ｊは１以上）だけ第８のステップに移って準備を行うよう回数を数える第１０のステップを備える。

【００３２】

更に、前記第５のステップにおいて、前記第１の出力結果と前記第２の出力結

果を比較した結果同一でなければ、前記第１のステップに戻って前記第１の出力結果と前記第２の出力結果を再び求め直すことが出来るように準備を行い、第１のステップに戻る第１１のステップを備える。

【００３３】

更に、前記第５のステップにおいて、前記第１の出力結果と前記第２の出力結果を比較した結果同一でなければ、予め定める一定回数ｓ回（ｓは１以上）だけ前記第１１のステップに移って準備を行うよう回数を数える第１２のステップを備える。

【００３４】

【発明の実施の形態】

本発明の実施の形態を例により説明する。

【００３５】

図１は、本発明による2重化システムの実施の形態の例である。先行系101と後続系102の二つのまったく同一な系を持つ。外部からの入力データは先行系101には直接入力されるが、後続系102には一旦入力データバッファ103に蓄えられた後、入力される。先行系101の出力結果は出力データバッファ104に蓄えられる。先行系正常終了検知・後続系開始制御部107において、先行系101が入力された入力データに対し、障害なく動作して出力結果が得られたかどうかを、監視している。先行系101が障害なく動作して正常に終了したことが確認されると、初めて後続系102に開始指示が出され、後続系102が入力データバッファ103に蓄えられた入力データにより動作を行う。後続系102の出力結果は出力結果比較器105により出力データバッファ104に蓄えられた先行系101の出力結果と比較される。比較した結果一致していれば、出力ゲート106が開いて後続系の出力結果が外部へ出力される。

【００３６】

図１において、先行系101に障害が発生し、与えられた入力データに対し正常終了しなかった時、先行系正常終了検知・後続系開始制御部107により制御され、後続系102は動作を開始しない。後続系102の内部状態が信号150により先行系101に複写され、先行系101は動作を開始する前の状態に回復される。このように

することで、先行系101に発生した障害が、コンピュータ・システムにおけるソフトウェアの障害であっても、障害回復を行うことができる。その後、先行系101は入力データ103に蓄えられていた入力データにより再び動作を開始することができる。

【００３７】

また出力比較器105において、比較した結果が一致していなかった時、出力ゲート106が制御されて、後続系102の出力結果は外部へ出力されない。このようにすることで、２重化システムとして、先行系101、後続系102の結果が一致した時のみ結果が出力されるので、外部に出力される結果の正当性を高めることができる。また不一致の時は誤った結果は出力されないので、誤った結果を外部に出力して悪影響を及ぼすことがない。更に先行系101、後続系102について不一致になった結果を再び求め直すように制御することも可能である。

【００３８】

図２は、図１の２重化システムの動作の様子を、横軸を時間として示した例である。ここで、ジョブA～ジョブDは、それぞれ一定の入力データに対し、先行系101、後続系102が結果を出力する単位であるとする。図２において、まずジョブAが先行系101で実行される。ジョブAが先行系101において正常に終了したことが確認されると、後続系102においてジョブAが実行される。後続系102においてジョブAが終了すると、その結果を、先に先行系101においてジョブAを実行した結果と比較する。比較した結果一致していれば、これを外部へ出力する。また先行系101は、後続系102においてジョブAが実行されている間に、次のジョブBを実行することが可能である。さらに先行系101においてジョブBが正常に終了すれば、この後、後続系102においてジョブBを実行するとともに、先行系101はその次のジョブCを実行することが可能である。

【００３９】

図２では、後続系102で1回目にジョブBを実行した結果が、先行系101でジョブBを1回目に実行した結果と一致しなかった時の動作を示している。この時、先行系101では既にジョブCを実行しておくことは可能ではあるが、ジョブCの後、再びジョブBに戻りジョブBの2回目の実行を行なう。先行系101においてジョブBの2

回目の実行が正常終了すると、再び後続系102においてジョブBの2回目の実行が行われる。図２では先行系101、後続系102におけるジョブBの2回目の実行の結果は一致した場合を示している。この場合、ジョブBの結果が、ここで初めて外部に出力される。また先行系101で次のジョブCが正常終了していれば、後続系102においても次のジョブCの実行が開始される。

【００４０】

図２では先行系101において、さらにその次のジョブDの実行が障害により異常終了した場合を示している。この時、異常報告を行ないながら、後続系102の状態を先行系101に複写することにより、先行系101の状態を回復することができる。

【００４１】

図３は、本発明による３重化システムの実施の形態の例である。３重化することにより、系１、系２、系３の三つの系の三つの結果がすべて一致してから初めて結果を外部に出力するようにすることができ、結果の正当性をさらに高めることができる。即ち、系１、系２、系3のそれぞれの単独の結果の正当性が低くても、外部に出力する結果の正当性は大きく高められる。また二つの先行系正常終了検知・後続系開始制御部１ 311及び先行系正常終了検知・後続系開始制御部２ 312を備え、系1が正常終了してから系2を、系２が正常終了してから系3を動作させるので、系３が正常終了する可能性も高められる。

【００４２】

図３では、ほとんどの動作は図１を自然に拡張した形で行われる。外部からの入力データは系1には直接入力されるが、系２及び系3には入力データバッファ304に一旦蓄えられてから入力される。系1の出力結果は出力データバッファ１ 305に蓄えられて、系2の出力結果と出力比較器306にて比較される。また系2の出力結果は同時に出力データバッファ２ 307に蓄えられ、系3の出力結果と出力比較器308にて比較される。二つの出力比較器306及び308の比較結果は出力一致検出・外部出力制御・再実行制御部309に入力され、二つの結果が両方とも一致であった時に、出力ゲート310が開かれて、系3の出力結果が外部へ出力される。

【００４３】

図３ではまた、系1が障害により正常終了しなかった時、先行系正常終了検知・後続系開始制御部１ 311により系2の動作開始が待機させられる。そして、系2の状態を系1へ複写することにより、系1の障害発生状態を消去し、状態回復を行なうことができる。同様に系2が障害により正常終了しなかった時、先行系正常終了検知・後続系開始制御部２ 312により系3の動作開始が待機させられ、系3の状態を系2へ複写して、系2の状態回復を行なうことができる。

【００４４】

図４は、本発明による３重化システムの別の実施の形態の例である。図１に示した２重化システムの例は、先行系及び後続系がそれぞれ正常終了していれば、出力比較器による比較結果が不一致であった場合には、再実行が可能であるとした例である。図４はこれに対し、それぞれの系が正常終了していても、結果が不一致であった時に再実行しようとすると、それぞれの系の状態を実行開始前に完全に復旧させる必要がある場合の例である。動作は次のようになる。

【００４５】

まず、外部から入力されたデータは系１には直接入力されるが、系２及び系３には入力データバッファ404に一旦蓄えられた後入力される。系1の出力結果は出力データバッファ405に蓄えられ、系2の出力結果と出力比較器406により一致しているかどうか比較される。比較した結果一致していれば出力ゲート407が開いて系2の結果が外部へ出力される。また先行系正常終了検知・後続系開始制御部１ 408により与えられた入力データに対し系1が正常終了することが確認されてから系2の動作を開始する。同様に先行系正常終了検知・後続系開始制御部２ 409により系２が正常終了することが確認され、かつ系１と系２の出力結果が出力比較器406において一致していたら、系３の動作を開始する。系３の出力結果は用いられず破棄される。系1が正常終了しなかった時には、先行系正常終了検知・後続系開始制御部１ 408により制御が行なわれ、系2の状態が系1へ複写され、系1の状態を復旧させる。その後、系1は入力データバッファ404に蓄えられた入力データにより再実行を行なうことができる。同様に系２が正常終了しなかった時には、先行系正常終了検知・後続系開始制御部２ 409により制御が行なわれ、系３の状態が系２へ複写され、系２の状態を復旧させる。系２も入力データバッ

ファ404に蓄えられた入力データにより再実行を行なうことができる。

【００４６】

また出力比較器406により比較した結果不一致であった時には、出力ゲート407が閉じられて外部には誤った結果は出力されない。この時、まだ実行前である系３の状態が系1及び系2の両方に複写され、系１、系2とも実行前の状態に復旧させることができる。図５に図４の動作を横軸に時間を取って示した例を掲げる。

【００４７】

図5において、ジョブA～ジョブGは図２と同様に、それぞれ一定の入力データについて系１、系2、系3が結果を出力する単位であるとする。図において、まずジョブAが系1において実行され、正常に終了することが確認されると、系２においてジョブAの実行が開始される。このとき同時に系1は次のジョブBの実行を行なうことが可能である。系２においてジョブAの実行が正常終了し、系１におけるジョブAの結果と比較した結果一致していれば、これを外部に出力する。また系３にて改めてジョブAの実行を開始させる。同時に系２は次のジョブBの実行を、系1は更にその次のジョブCの実行を開始することが可能である。

【００４８】

図5では、系1、系2におけるジョブBの１回目の実行結果が不一致であった場合を示している。この時、系３でのジョブBの実行開始を行なわない。そして系３が持つジョブAの終了直後(ジョブBの実行開始前)の状態を系１、系２の両方に複写して、系１、系２の両方ともジョブB実行開始前の状態に戻す。その後、系１、系2において再びジョブBを実行する。図５では系１、系2におけるこの2回目のジョブBの実行で、結果が一致した場合を示している。系１、系2の結果が一致して初めて系3でジョブBの実行開始を行う。

【００４９】

図5では、さらにその後、系１におけるジョブDの実行で、障害が発生し、異常終了した場合を示している。この時、系２は直前のジョブCの実行を終了した状態で、ジョブDの実行開始を行わない。そして系２の状態を系１に複写することによって、系１の状態をジョブDの実行開始前の状態に回復させる。図５では、その後系１において再びジョブDの実行を行い、この２回目のジョブDの実行では

障害が発生せずに正常終了した場合を示している。このような動作は図２における後半部分のジョブDの実行の様子と同様である。

【００５０】

図６は、本発明による２重化システムについて、さらに先行系601、後続系602がそれぞれCPU 610及び612、メインメモリ 611及び613からなるコンピュータ・システムである場合の実施の形態の例である。図６において、外部からの入力データは先行系601には直接入力され、後続系602には一旦入力データバッファ603に蓄えられた後、入力される。先行系601の出力結果は出力データバッファ604に蓄えられる。先行系正常終了監視部607において、先行系601が障害なく動作して出力結果が得られるかどうかの監視を行っている。先行系601において障害なく出力結果が得られた場合には、それを後続系開始制御部608に通知し、後続系開始制御部608において後続系602に実行開始指示を送出する。後続系602が実行を開始して得られた出力結果は、出力データバッファ604に蓄えられた先行系601の出力結果と、出力比較器605において比較される。出力比較器605における比較において、両者の出力結果が一致している場合には出力ゲート606が開かれ、後続系602の出力結果が外部へ出力される。

【００５１】

先行系正常終了監視部607の監視結果において、先行系601で障害が発生し、出力結果が得られなかった場合には、後続系開始制御部608による後続系602の実行開始指示は出力されず、後続系602は実行を開始しないで待機状態となる。そして先行系正常終了監視部607よりメモリコピー制御部609へ先行系601の状態回復指示が送出される。メモリコピー制御部609では、先行系601の状態回復指示を受け取ると、後続系602のメインメモリ613の内容を先行系601のメインメモリ611へ複写し、先行系601の状態回復を行う。更にこのとき、後続系602のCPU 612の内部状態を先行系601のCPU 610へ複写すれば、CPU 610の内部状態を含め、先行系601の状態を完全に回復させることもできる。このようにすることによって、先行系601において、ソフトウェア障害を含む障害が発生しても、CPU 610及びメインメモリ611の状態を回復させることが可能である。

【００５２】

図７は、図４で更に系１ 701、系2 702、系3 703がそれぞれCPU 710、 712及び714、メインメモリ711、713及び715からなるコンピュータ・システムである場合の、本発明による3重化システムの実施の形態の例である。図７において、外部からの入力データは系1には直接入力されるが、系２、系３については、一旦入力データバッファ704に蓄えられた後、入力される。系１の出力結果は出力データバッファ705に蓄えられる。系1正常終了監視部716において、系１が障害なく動作して出力結果が得られるかどうかを監視している。系1において障害なく出力結果が得られた場合には、それを系2開始制御部717に通知し、系２開始制御部717において系２に実行開始指示を送出する。系２が実行を開始して得られた出力結果は、出力データバッファ705に蓄えられた系１の出力結果と、出力比較器706において比較される。出力比較器706での比較において両者の出力結果が一致している場合には、外部出力制御・再実行制御部707において出力ゲート708が開かれて、系２の出力結果が外部へ出力される。更に系２正常終了監視部719において、系2が障害なく動作して出力結果が得られるかどうかを監視している。系2において障害なく出力結果が得られた場合には、それを系3開始制御部720に通知する。系3開始制御部720では、系２正常終了監視部719から系2が障害なく動作して出力結果が得られたことの通知、及び外部出力制御・再実行制御部707よりの系１、系２の出力結果が一致したことの通知を受け、両方の通知が揃うと、系3に実行開始指示を送出する。系３では実行を開始すると、入力データバッファ704より入力データを受信し、CPU 714、メインメモリ715の状態を変更する。系3の出力結果は用いられずに破棄される。

【００５３】

系1正常終了監視部716の監視結果において、系1で障害が発生し、出力結果が得られなかった場合には、系２開始制御部717による系2の実行開始指示は出力されず、系２は実行を開始しないで待機状態となる。そして系1正常終了監視部716により系1-2メモリコピー制御部718へ系１の状態回復指示が送出される。系1-2メモリコピー制御部718では、系１の状態回復指示を受け取ると、系２のメインメモリ713の内容を系1のメインメモリ711へ複写し、系1の状態回復を行う。更にこのとき、系2のCPU 712の内部状態を系１のCPU 710へ複写すれば、CPU 710の内

部状態を含め、系１の状態を完全に回復させることができる。同様に、系2正常終了監視部719の監視結果において、系2で障害が発生し、出力結果が得られなかった場合には、系３開始制御部720による系3の実行開始指示は出力されず、系3は実行を開始しない。そして系2正常終了監視部719により系2-3メモリコピー制御部721へ系２の状態回復指示が送出される。系2-3メモリコピー制御部721では、系２の状態回復指示を受け取ると、系３のメインメモリ715の内容を系２のメインメモリ713へ複写し、系２の状態回復を行う。

【００５４】

また出力比較器706において、系１と系2の出力結果が一致しなかった時、外部出力制御・再実行制御部707において、外部出力ゲート708が閉じられて、一致しなかった出力結果は外部へ出力されない。更に、系3開始制御部720は系3への実行開始指示を送出せず、系３は待機状態となる。この時、外部出力制御・再実行制御部707は、系2-3メモリコピー制御部721及び系3-1メモリコピー制御部722に系２、系１の状態回復指示を送出する。系2-3メモリコピー制御部721、系3-1メモリコピー制御部722は系3のメインメモリ715の内容をそれぞれ、系２のメインメモリ713、系１のメインメモリ711へ複写し、系２、系１の状態回復を行う。この時、系３のCPU 714の内部状態を系２のCPU 712及び系１のCPU 710へ複写し、系２、系１の状態をCPUの内部状態を含め、完全に回復させることも可能である。以上のような動作によって、系１、系２でソフトウェア障害を含む障害が発生した場合、及び系１と系２の出力結果が不一致であった場合、系１、系２の状態を正しく回復させることができる。

【００５５】

図8は、本発明による信頼性を高める方法の実施の例である。図８において、ステップ801において、入力されたデータより第1の出力結果を求める。次にステップ802において、第1の出力結果が障害なく求まったかどうか判断する。障害なく求まったときにはステップ803に進む。障害があったときにはステップ808に進み、予め定めるｋ回(ｋは１以上)繰り返し第1の結果を求めようとしたどうか判断する。まだｋ回繰り返していなければ、ステップ809に達し、第1の出力結果を再び求め直すように準備して、ステップ801に戻る。ｋ回繰り返していれば、ス

テップ814に達し障害報告を行って障害終了とする。

【００５６】

ステップ803では、入力された同じデータより第2の出力結果を求める。次にステップ804において第2の出力結果が障害なく求まったかどうか判断する。障害なく求まった時にはステップ805に進む。障害があったときにはステップ810に進み、予め定めるｊ回(ｊは１以上)繰り返し第２の結果を求めようとしたどうか判断する。まだｊ回繰り返していなければ、ステップ811に達し、第２の出力結果を再び求め直すように準備して、ステップ803に戻る。ｊ回繰り返していれば、ステップ814に達し障害報告を行って障害終了とする。

【００５７】

ステップ805では、第１と第2の出力結果の比較を行う。次にステップ806において比較した結果一致したどうか判断する。一致していればステップ807に進み、第１または第2の出力結果を出力して正常終了とする。一致していなければ、ステップ812に進み、予め定めるｓ回(ｓは１以上)繰り返したかどうか判断する。まだｓ回繰り返していなければ、ステップ813に進み、第1と第2の出力結果の両方を求め直すための準備を行い、ステップ801に戻る。ｓ回繰り返していれば、ステップ814に達し障害報告を行って障害終了とする。以上のようにすることによって、障害なく得られた二つの出力結果を更に比較して一致した時に結果出力を行うので、出力結果の信頼性を高めることができる。

【００５８】

図９は、図６に示した本発明によるコンピュータ・システムの2重化システムの実施の形態の例について、更に縮退運転制御部914を付加した例である。縮退運転制御部914では、通常は出力比較器905の比較結果によって、そのまま出力ゲート906を制御している。また先行系正常終了監視部907より先行系901が障害なく動作しているかどうかの報告を受ける。先行系正常終了監視部907では、図６と同様に先行系901が障害なく動作して結果が得られているかどうか監視しており、障害が発生した場合にはメモリコピー制御部909に先行系901の状態回復を指示する。しかし、予め定める一定回数状態回復を行っても先行系901より障害なく結果が得られなくなると、これを縮退運転制御部914に通知する。縮退運転制

御部914では、この通知を受けると、後続系開始制御部908に、先行系正常終了監視部907からの先行系が障害なく動作したかどうかの通知と関係なく後続系902に実行開始指示を送出するように指示する。同時に出力比較器905の比較結果に関わらず出力ゲート906を開くように制御を行って、後続系902の出力結果をそのまま外部に出力する。さらに入力データバッファ903を制御し、外部から入力されたデータを入力データバッファ903内で蓄えずに後続系902にそのまま入力させるようにして、入力データバッファ903に一旦蓄えることによる後続系902へのデータ入力の遅延も削除することが可能である。このようにすることによって、先行系901が何らかの障害によって、動作を回復し継続することが不可能になっても、後続系902だけで処理を続けることが可能であり、可用性を高めることができる。図９のほかの動作は図６と同じである。

【００５９】

図１０は、再び図６に示した本発明によるコンピュータ・システムの2重化システムの実施の形態の例について、更に後続系正常終了監視部214を付加し、メモリコピー制御部609の代わりに双方向メモリコピー制御部209を、出力ゲート606の代わりにセレクタ付き出力ゲート206を設けた例である。後続系正常終了監視部214では、後続系202が障害なく動作して結果が出力されているかどうか監視している。後続系202で障害が発生したことが検出されると、後続系開始制御部208に信号を送り、一旦後続系開始制御部208からの実行開始指示を抑制する。次に双方向メモリコピー制御部209に信号を送り、先行系201のメインメモリ211の内容を後続系202のメインメモリ213に複写し、後続系202の状態を先行系201の状態と同一することによって、状態回復を行う。この時、先行系201で既に出力されて出力データバッファ204に蓄えられている出力結果と比較すべき出力結果は後続系202よりもはや出力されない。このため、セレクタ付き出力ゲート206を制御して、出力データバッファ204に蓄えられている先行系201の出力結果をそのまま外部に出力する。このようにすることによって、後続系202において障害が発生しても、後続系202の状態を回復し、さらに出力も途切れさせずに処理を継続させることが可能である。図１０のほかの動作は図６と同様である。

【００６０】

図１１は、図６の先行系正常終了監視部607、図７の系1正常終了監視部716及び系２正常終了監視部719、図９の先行系正常終了監視部907、図１０の先行系正常終了監視部207として用いることのできる正常終了監視部507について、さらに内部を詳細化した例である。図１１において、正常終了監視部507は、CPU 502、メインメモリ503からなる系501が障害なく動作し、結果を出力するかどうか監視している。図で、データ入力があると、結果出力監視部508が監視動作を開始し、タイマー部509にタイマーカウントの開始を指示する。結果出力監視部508は次に系501の結果出力を監視し、結果が出力されるのを待つ。もし系501の結果出力が行われる前にタイマー部509において予め定めたカウント値に達したことが通知されると、結果出力監視部508はタイムアウトによる障害検出と判断し、障害監視結果集計制御部510にタイムアウト障害を報告する。タイマー部509において予め定めたカウント値に達する前に結果出力が行われれば、結果出力監視部508はタイマー部509にリセット指示を送り、タイマー部509のタイマーカウント動作を停止させる。同時に障害監視結果集計制御部510に障害なく結果出力が行われたことを通知する。また、不正アドレス参照監視部506は、CPU 502が行うメインメモリ503に対する参照アドレスの監視を行い、系501によって定まる正当なアドレスの範囲を超えるアドレスの参照があった場合には、不正アドレス参照による障害検出と判断し、障害監視結果集計制御部510に報告する。CPU命令実行障害監視部505は、CPU 502の命令実行動作を監視し、CPU 502において命令の実行に障害が発生したり、命令の実行の結果例外事象が発生したりすると、これを検知して、CPU命令実行における障害検出と判断して障害監視結果集計制御部510に報告する。メモリデータ障害監視部507は、同様にメインメモリ503への読み出し・書き込み動作を監視し、読み出し・書き込み動作における障害発生を検知して、これを障害監視結果集計制御部510に報告する。障害監視結果集計制御部510では、CPU命令実行障害監視部505、不正アドレス参照監視部506、メモリデータ障害監視部507、結果出力監視部508より障害発生の報告を受ける。障害が発生した場合には、障害回復制御部511へ制御信号を伝達し、状態回復信号520を送出させて、系501の状態回復を行わせる。また障害発生の報告がなく、結果出力監視部508より障害なく結果出力が行われたことが通知されたら、無障害確認制御部512に制

御信号を伝達し、無障害確認信号521を送出させる。以上のような動作により、系501が障害なく結果を出力できたかどうかを監視することができる。

【００６１】

図１２は、本発明による2重化システムの別の実施の形態の例である。図１２では、先行系121、後続系122の2個の系を持つが、出力については、先行系121の出力結果をそのまま外部に出力しており、2個の系の出力結果の比較は行わない。図１２で、外部からの入力データは、先行系121には直接入力されるが、後続系122には一旦入力データバッファ123に蓄えられた後、入力される。先行系正常終了検知・後続系開始制御部127において、先行系121が入力された入力データに対し、障害なく動作して出力結果が得られたかどうかを、監視している。先行系121が障害なく動作して正常に終了したことが確認されると、初めて後続系122に開始指示が出され、後続系122が入力データバッファ123に蓄えられた入力データにより動作を行う。後続系122の出力結果は破棄される。

【００６２】

図１２において、先行系121に障害が発生し、与えられた入力データに対し正常終了しなかった時、先行系正常終了検知・後続系開始制御部127により制御され、後続系122は動作を開始しない。後続系122の内部状態が信号151により先行系121に複写され、先行系121は動作を開始する前の状態に回復される。このようにすることで、先行系121に発生した障害が、コンピュータ・システムにおけるソフトウェアの障害であっても、障害回復を行うことができる。その後、先行系121は入力データバッファ123に蓄えられていた入力データにより再び動作を開始することができる。図１に示した例にくらべ、出力結果の正当性については高められないが、出力データバッファ104、出力比較器105、出力ゲート106を必要としないので、ソフトウェア障害を含む障害回復を行うシステムを簡単に構成することが可能である。さらに図１２では、先行系121の出力結果をそのまま外部に出力するので、出力が外部に行われるまでの時間の遅延がない。

【００６３】

図１３に、本発明による2重化システムのさらに別の実施の形態の例を掲げる。図１３は、図１２に示した例と同じく、出力については、2個の系の出力結果

の比較を行っていない。図１３では、後続系132の出力結果をそのまま外部に出力している。先行系131の出力結果は破棄される。ほかの動作は図１２と同様である。図１２に比べ、後続系132の出力結果を用いているため、出力が外部に行われるまでの時間の遅延は存在する。しかし、先行系131が与えられた入力データに対し障害なく動作することが確認されてから出力が行われるので、出力が得られることに対する信頼性は高められる。また、図１２の例と同じく、図１に比べて出力データバッファ104、出力比較器105、出力ゲート106を必要としないので、ソフトウェア障害を含む障害回復を行うシステムを簡単に構成することができる。

【００６４】

【発明の効果】

本発明により、多重化による出力結果の信頼性向上に加え、障害を起こした系の状態を正しく復旧させることができる。また障害発生時に外界への出力を抑制し、外界に悪影響を及ぼすことを避けることが可能である。特にシステムが動作を規定するソフトウェアを持つコンピュータ・システムである場合には、当該ソフトウェアの不良も含むソフトウェア障害が生じても、正しく状態回復を行うことができる。

【図面の簡単な説明】

【図１】

本発明の一実施例である２重化システムのブロック図である。

【図２】

上記実施例の２重化システムの動作を説明する図である。

【図３】

本発明の別の実施例である３重化システムを示すブロック図である。

【図４】

本発明の更に別の実施例の３重化システムを示すブロック図である。

【図５】

上記実施例の３重化システムの動作を説明する例である。

【図６】

本発明の更に別の実施例の２重化システムを示すブロック図である。

【図７】

本発明の更に別の実施例の３重化システムを示すブロック図である。

【図８】

更に信頼性を高める実施例の処理方法を示すフローチャートである。

【図９】

本発明の更に別の実施例の縮退運転制御部を備えた２重化システムを示すブロック図である。

【図１０】

本発明の更に別の実施例の後続系正常終了監視部を備えた２重化システムを示すブロック図である。

【図１１】

各実施例の正常終了監視部を詳細に示すブロック図である。

【図１２】

本発明の更に別の実施例の２重化システムを示すブロック図である。

【図１３】

本発明の更に別の実施例の２重化システムを示すブロック図である。

【符号の説明】

101、201、601、901、121、131 ..... 先行系

102、202、602、902、122、132 ..... 後続系

301、401、701 ..... 系１

302、402、702 ..... 系２

303、403、70..... 系３

103、203、304、404、603、704、903、123、133 .... 入力データバッファ

104、405、604、705、904 ..... 出力データバッファ

305 ..... 出力データバッファ１

307 ..... 出力データバッファ２

105、205、306、308、406、605、706、905 ..... 出力比較器

106、310、407、606、708、906 ..... 出力ゲート

206 ..... セレクタ付き出力ゲート

107、127、137 ..... 先行系正常終了検知・後続系開始制御部

311、408 ..... 先行系正常終了検知・後続系開始制御部1

312、409 ..... 先行系正常終了検知・後続系開始制御部2

309 ..... 出力一致検出・外部出力制御・再実行制御部

707 ..... 外部出力制御・再実行制御部

914 ..... 縮退運転制御部

214 ..... 後続系正常終了監視部

210、212、502、610、612、710、712、714、910、912 ..... CPU

211、213、503、611、613、711、713、715、911、913 ..... メインメモリ

207、607、907 ..... 先行系正常終了監視部

716 ..... 系1正常終了監視部

719 ..... 系２正常終了監視部

208、608、908 ..... 後続系開始制御部

717 ..... 系２開始制御部

720 ..... 系３開始制御部

609、909 ..... メモリコピー制御部

718 ..... 系1-2メモリコピー制御部

721 ..... 系2-3メモリコピー制御部

722 ..... 系3-1メモリコピー制御部

209 ..... 双方向メモリコピー制御部

505 ..... CPU命令実行障害監視部

506 ..... 不正アドレス参照監視部

507 ..... メモリデータ障害監視部

508 ..... 結果出力監視部

509 ..... タイマー部

510 ..... 障害監視結果集計制御部

511 ..... 障害回復制御部

512 ..... 無障害確認制御部

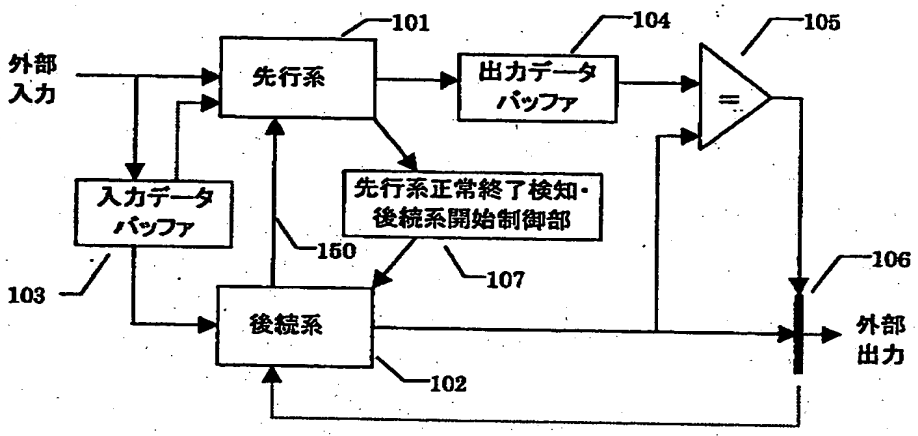
520 ..... 状態回復信号

521 ..... 無障害確認信号。

【書類名】　図面

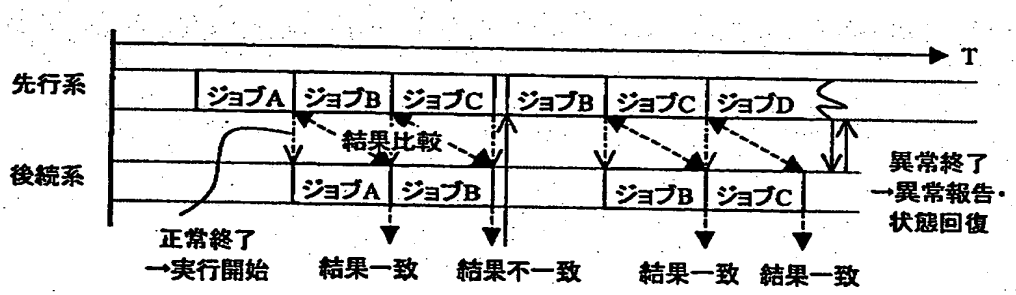
【図１】

図1



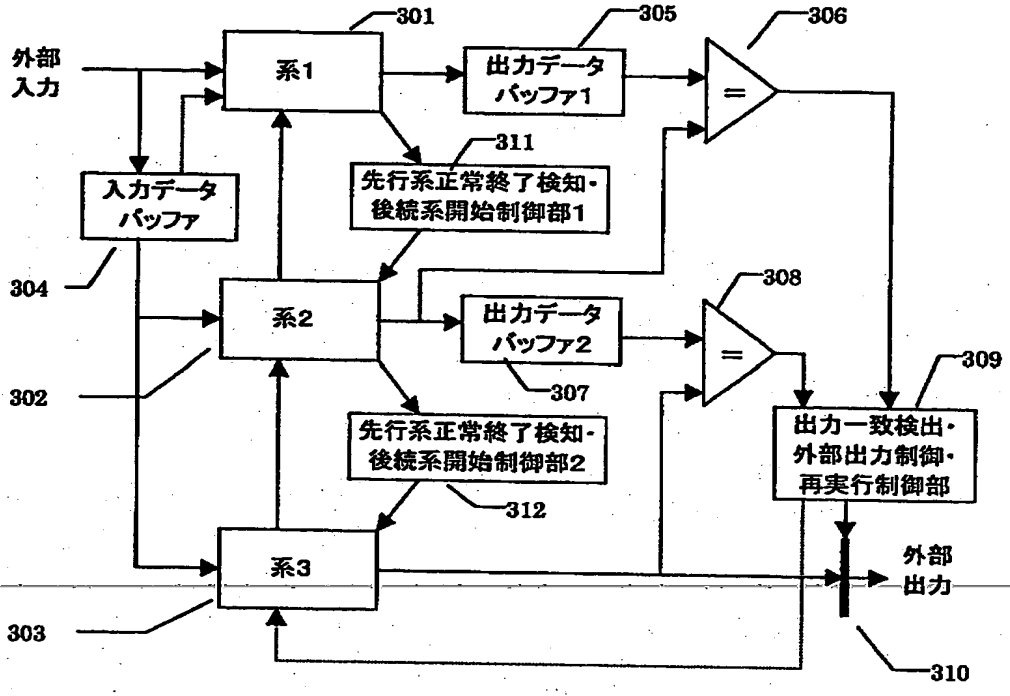
【図２】

図2



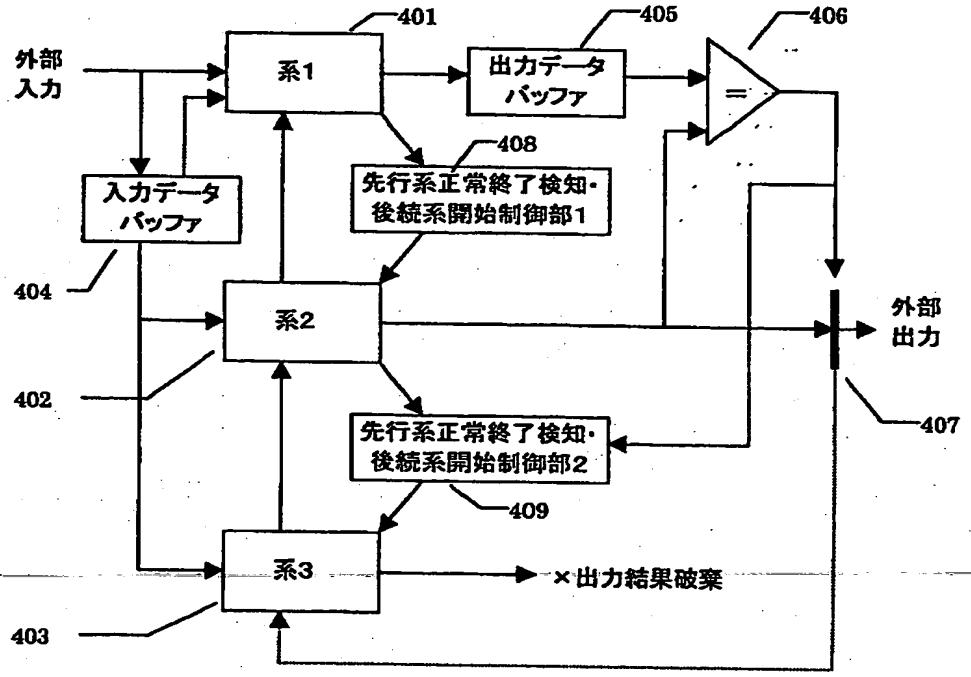
【図３】

図3


外部
入力
系1
301
出力データ
バッファ1
305
=
306
入力データ
バッファ
304
311
先行系正常終了検知・
後続系開始制御部1
系2
出力データ
バッファ2
308
=
309
302
307
先行系正常終了検知・
後続系開始制御部2
312
出力一致検出・
外部出力制御・
再実行制御部
系3
外部
出力
303
310

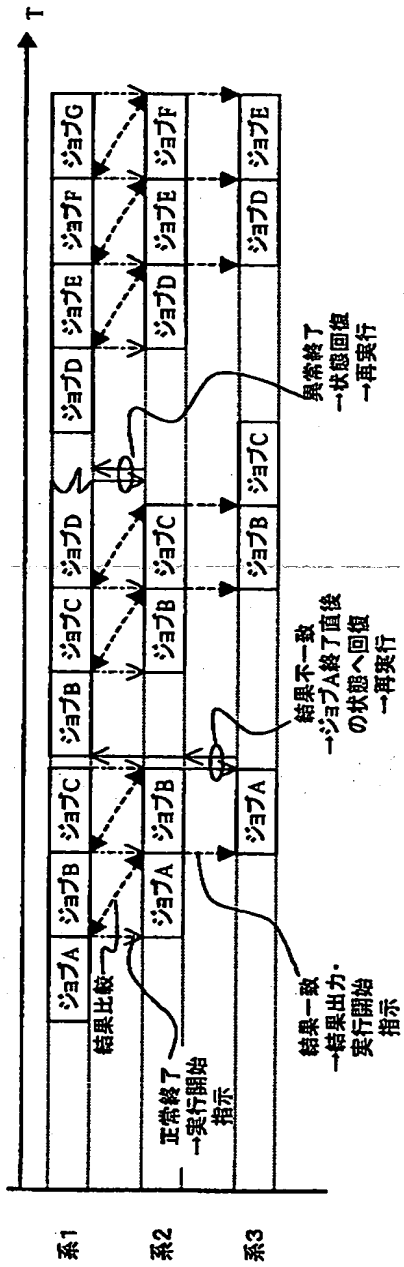
【図４】

図4


外部
入力
系1
401
出力データ
バッファ
405
406
=
入力データ
バッファ
404
先行系正常終了検知・
後続系開始制御部1
408
系2
402
外部
出力
407
先行系正常終了検知・
後続系開始制御部2
409
系3
×出力結果破棄
403

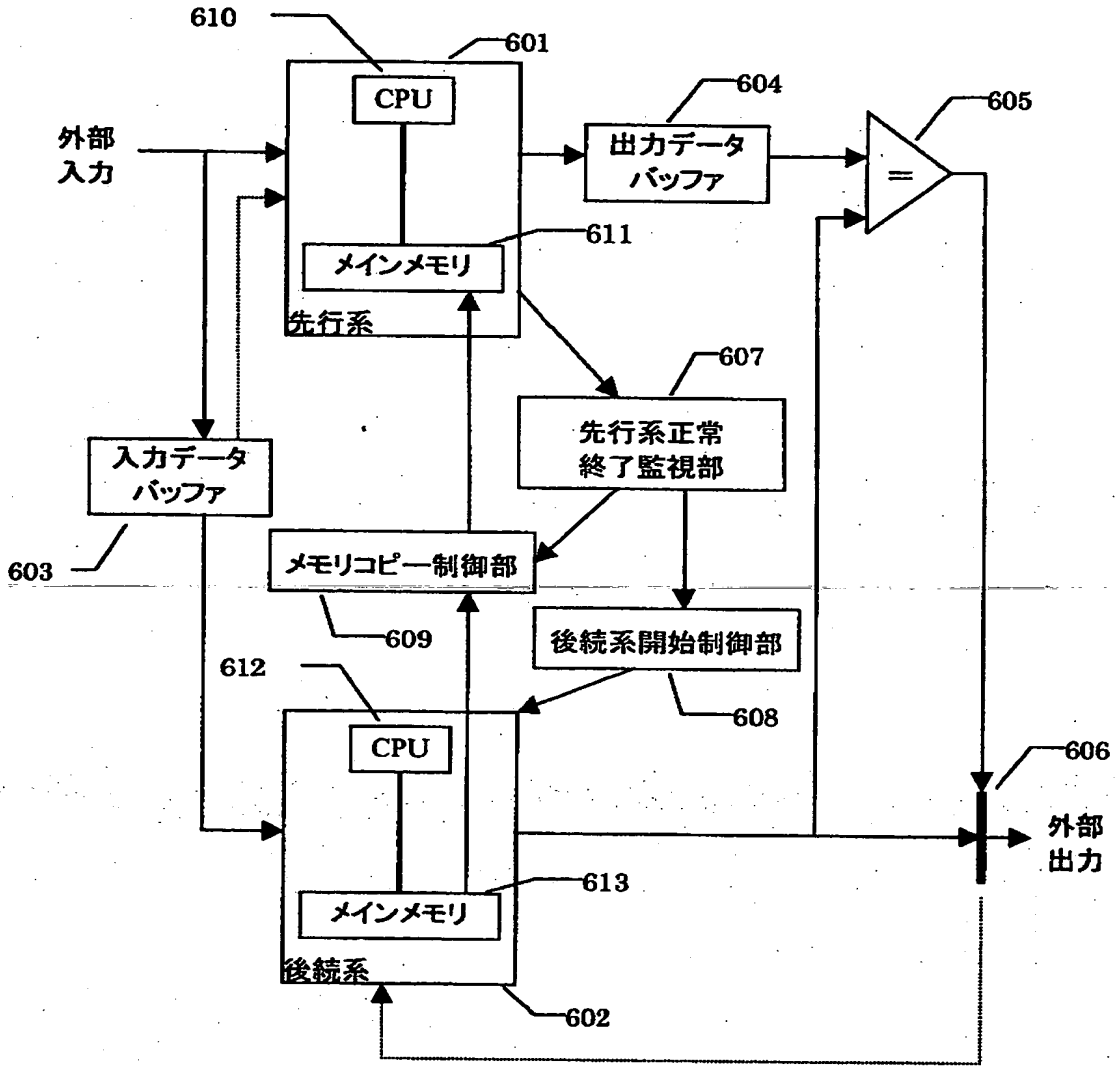
【図５】

図5


T
ジョブA
ジョブB
ジョブC
ジョブD
ジョブE
ジョブF
ジョブG
結果比較
正常終了
→実行開始
指示
結果一致
→結果出力・
実行開始
指示
結果不一致
→ジョブA終了直後
の状態へ回復
→再実行
異常終了
→状態回復
→再実行
系1
系2
系3

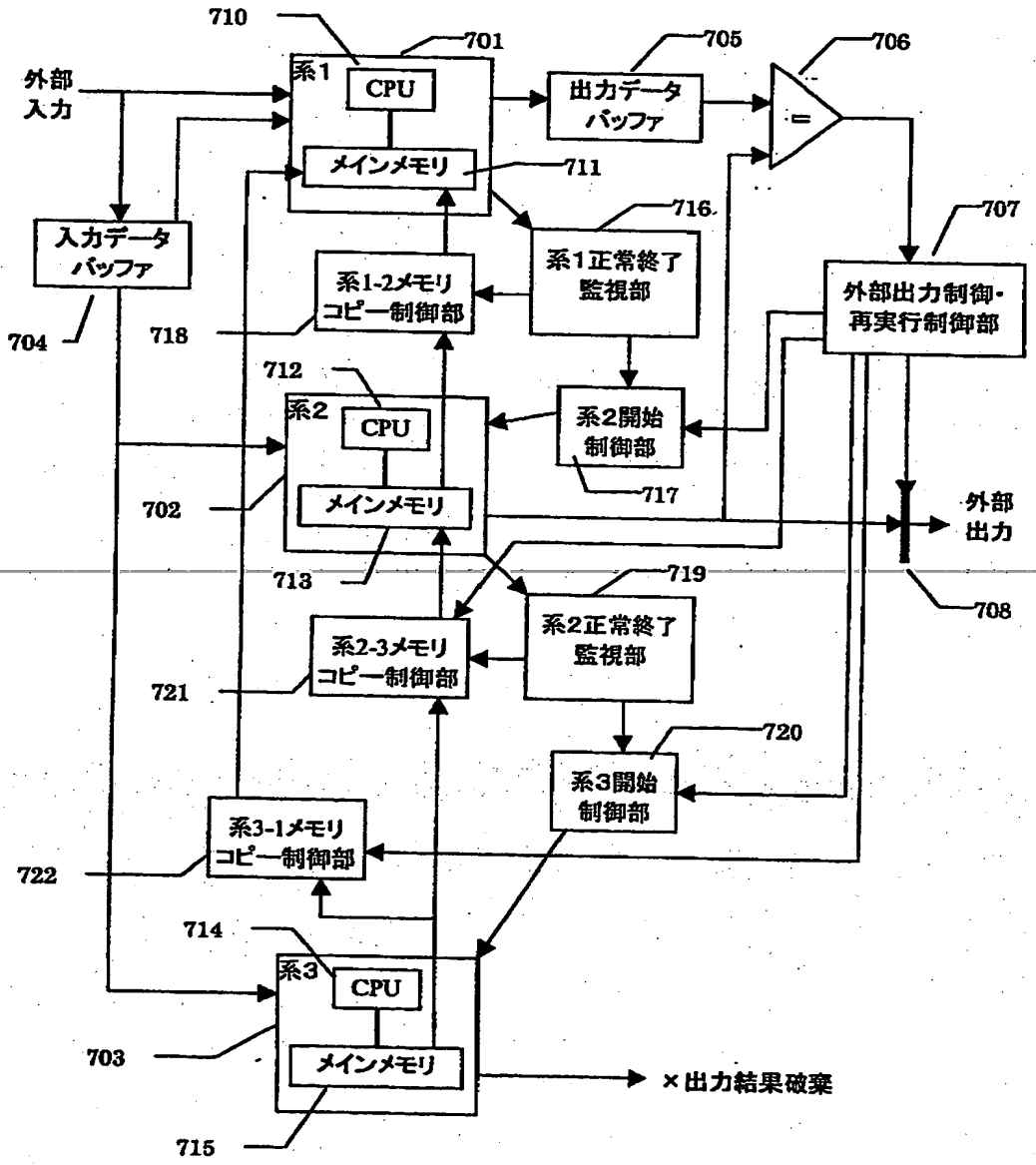
【図６】

図6


610
601
CPU
604
605
外部
入力
出力データ
バッファ
=
611
メインメモリ
先行系
607
先行系正常
終了監視部
入力データ
バッファ
603
メモリコピー制御部
609
後続系開始制御部
612
608
CPU
606
外部
出力
613
メインメモリ
後続系
602

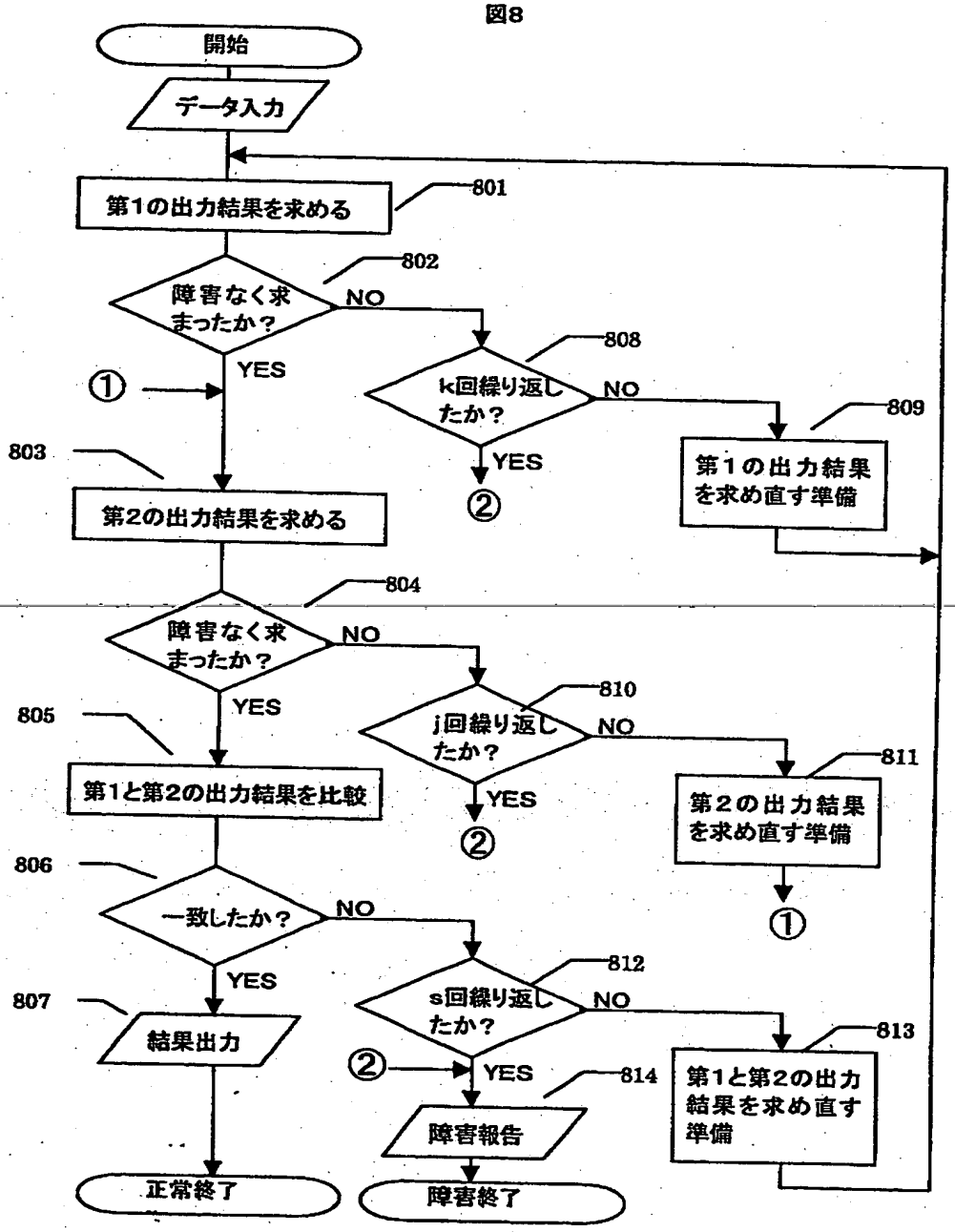
【図７】

図7


710
701
系1
CPU
メインメモリ
711
外部
入力
入力データ
バッファ
704
705
出力データ
バッファ
706
=
707
716
系1正常終了
監視部
系1-2メモリ
コピー制御部
718
外部出力制御・
再実行制御部
712
系2
CPU
メインメモリ
702
713
系2開始
制御部
717
外部
出力
708
719
系2正常終了
監視部
系2-3メモリ
コピー制御部
721
720
系3開始
制御部
系3-1メモリ
コピー制御部
722
714
系3
CPU
メインメモリ
703
715
×出力結果破棄

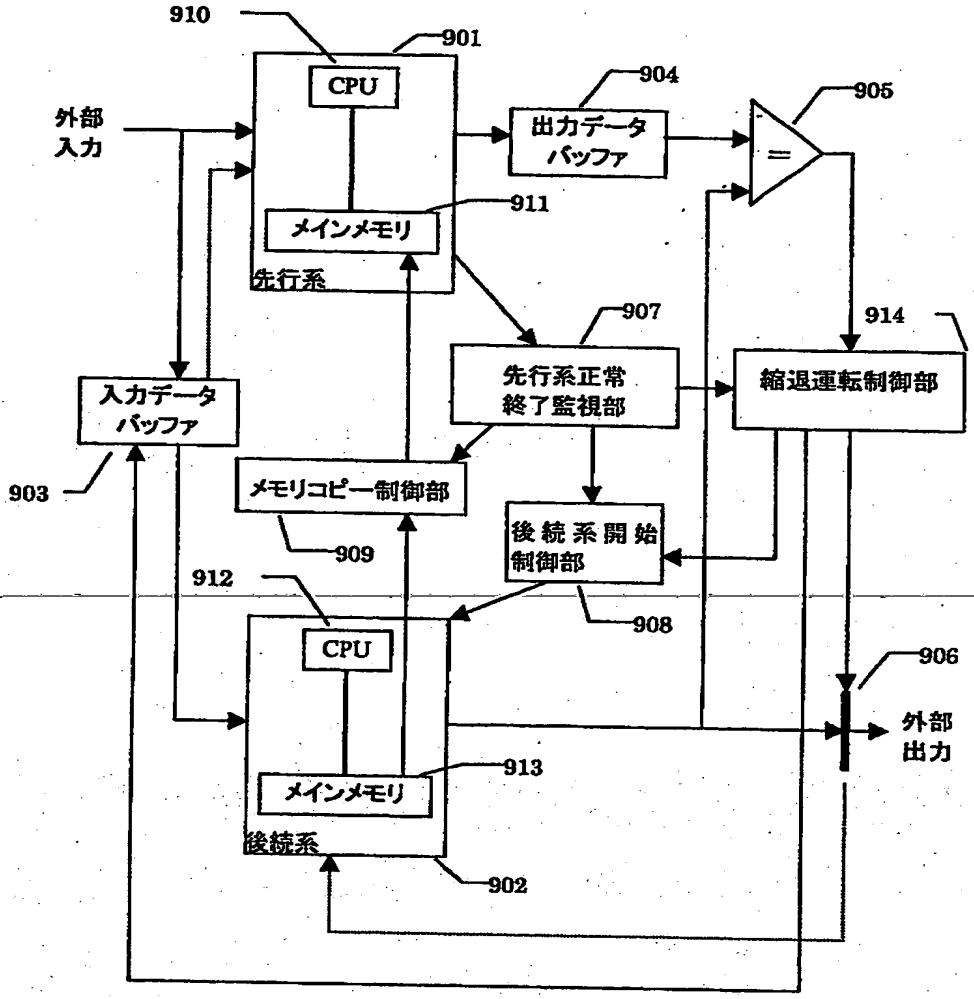
【図８】

図8


開始
データ入力
第1の出力結果を求める
801
障害なく求まったか？
802
NO
YES
①
k回繰り返したか？
808
NO
YES
②
809
第１の出力結果を求め直す準備
803
第2の出力結果を求める
障害なく求まったか？
804
NO
YES
805
第1と第2の出力結果を比較
j回繰り返したか？
810
NO
YES
②
811
第２の出力結果を求め直す準備
①
806
一致したか？
NO
YES
807
結果出力
s回繰り返したか？
812
NO
②
YES
814
障害報告
813
第1と第2の出力結果を求め直す準備
正常終了
障害終了

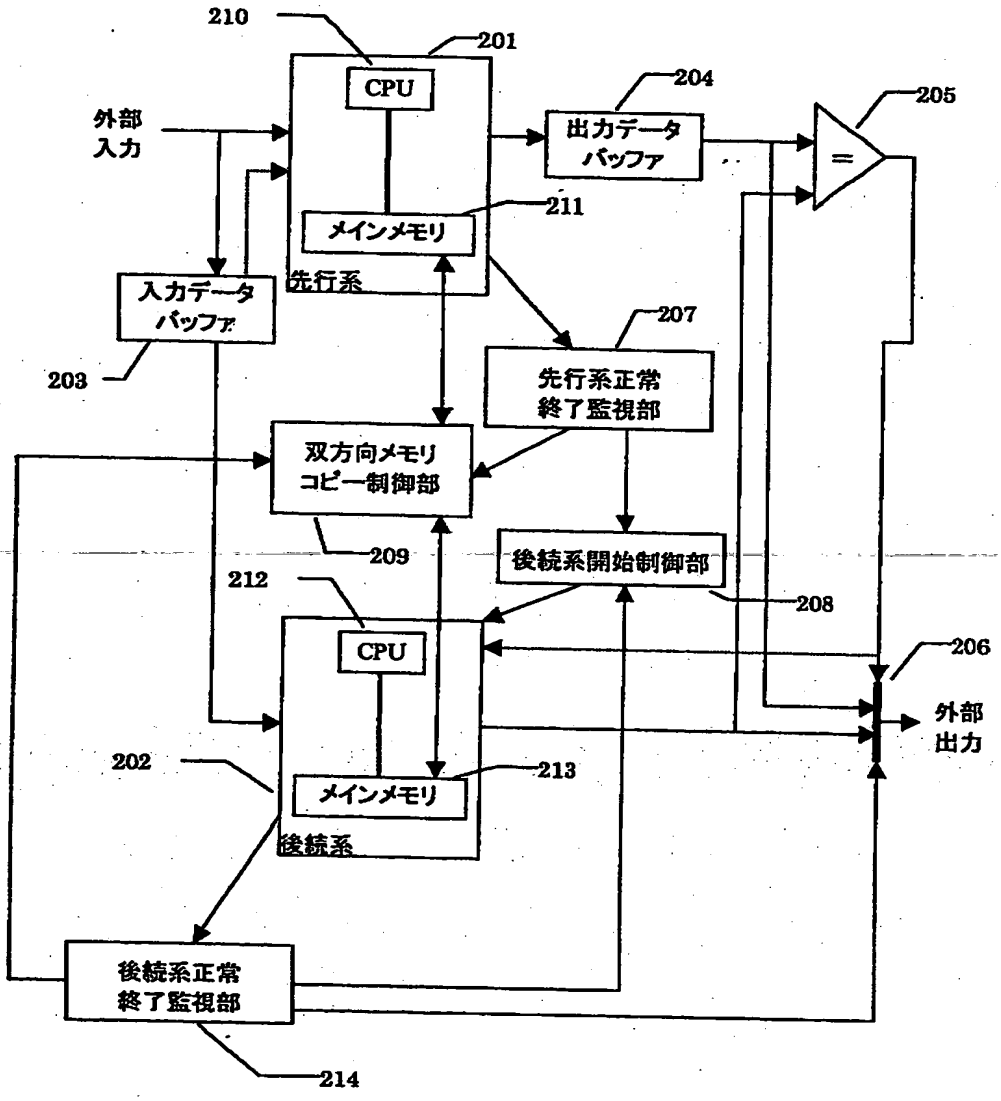
【図９】

図9


910
901
CPU
外部
入力
904
出力データ
バッファ
905
=
911
メインメモリ
先行系
907
914
先行系正常
終了監視部
縮退運転制御部
入力データ
バッファ
903
メモリコピー制御部
909
後続系開始
制御部
912
908
CPU
906
外部
出力
913
メインメモリ
後続系
902

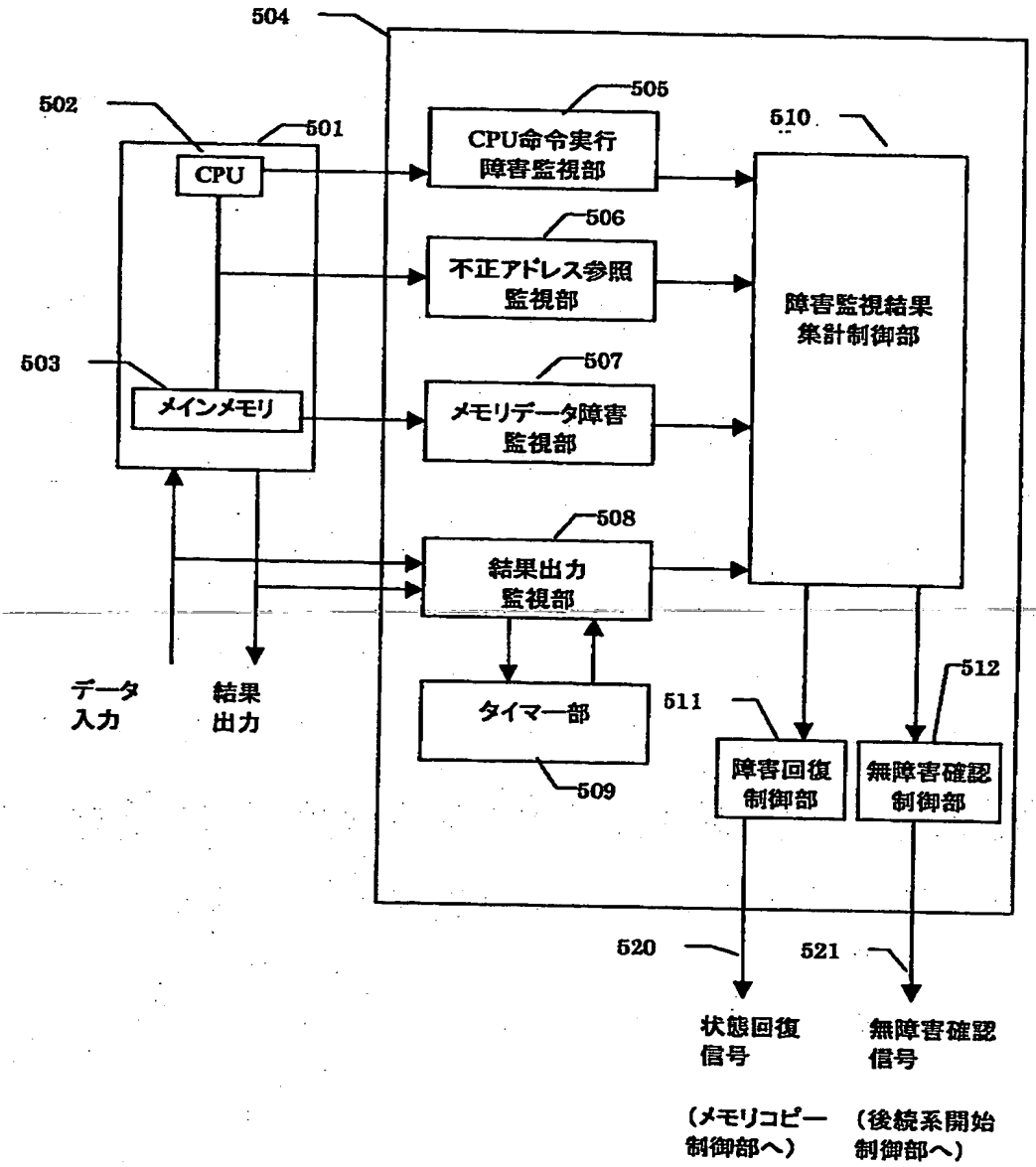
【図１０】

図10


210
201
CPU
204
205
外部
入力
出力データ
バッファ
=
211
メインメモリ
先行系
入力データ
バッファ
207
203
先行系正常
終了監視部
双方向メモリ
コピー制御部
209
後続系開始制御部
212
208
CPU
206
外部
出力
202
213
メインメモリ
後続系
後続系正常
終了監視部
214

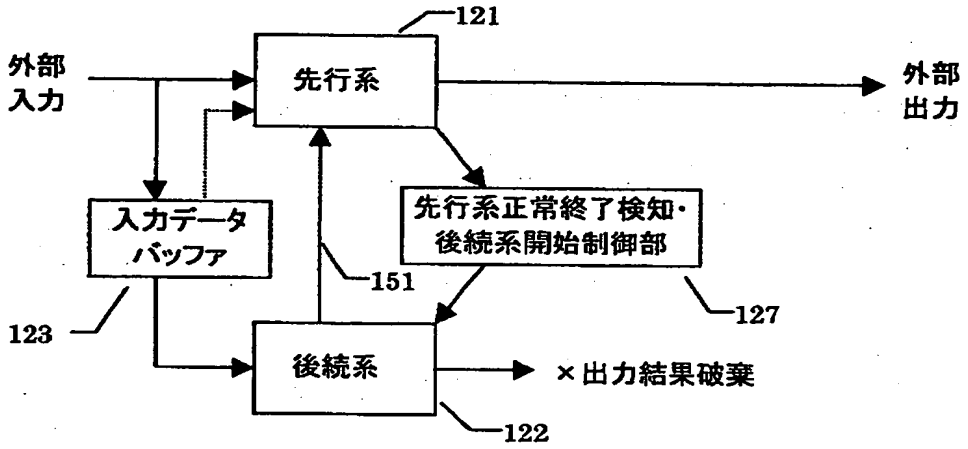
【図１１】

図11


504
502
501
CPU
505
CPU命令実行
障害監視部
510
506
不正アドレス参照
監視部
障害監視結果
集計制御部
503
メインメモリ
507
メモリデータ障害
監視部
508
結果出力
監視部
データ
入力
結果
出力
タイマー部
511
512
障害回復
制御部
無障害確認
制御部
509
520
521
状態回復
信号
無障害確認
信号
（メモリコピー
制御部へ）
（後続系開始
制御部へ）

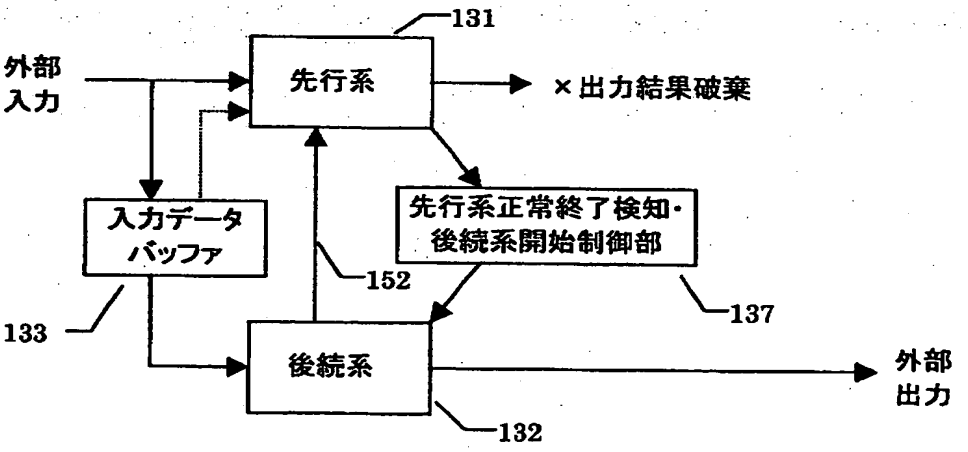
【図１２】

図12



【図１３】

図13



【書類名】　要約書

【要約】

【課題】多重化システムにおいて、ハードウェアの障害や誤動作に加え、ソフトウェアの不良を含むソフトウェア障害についても正しく状態回復を行う。

【解決手段】先行系101、後続系102の二つの系を備え、入力データを先行系101には直接入力して動作させる。後続系102は入力データを入力データバッファ103に一旦蓄え、先行系101が与えられた入力データについて障害なく出力結果が得られることを先行系正常終了検知・後続系開始制御部107において確認してから、入力データバッファ103に蓄えた入力データを読み出して動作を開始する。先行系101の出力結果は出力データバッファ104に蓄えられ、後続系102より出力結果が得られてから出力比較器105で一致しているかどうか比較し、一致していれば出力ゲート106を開いて外部に出力する。先行系101で障害が発生した場合には、後続系102の状態を複写することで先行系101の状態回復を行う。

【効果】後続系102で常に動作前の状態を保持しているため、ソフトウェア障害を含む障害が発生しても先行系101の状態を動作前の状態に回復することができる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００１－１９５６８７
受付番号	５０１００９４０９１１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１３年　６月２９日

＜認定情報・付加情報＞

【提出日】　平成13年 6月28日

次頁無

出証特２００２－３０１１６６５

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所